On solving L P N using B K W and variants

DOI: 10.1007/s12095-015-0149-2
Cryptography and Communications, 2016, 8, 331-369.

#	Paper	IF	Citations
19	How to Sequentialize Independent Parallel Attacks?. *Lecture Notes in Computer Science*, **2015**, 704-731	0.9	1
18	On Iterative Collision Search for LPN and Subset Sum. *Lecture Notes in Computer Science*, **2017**, 729-746	0.9	4
17	Efficient Authentication from Hard Learning Problems. *Journal of Cryptology*, **2017**, 30, 1238-1275	2.1	5
16	Key-Recovery Attacks on ASASA. *Journal of Cryptology*, **2018**, 31, 845-884	2.1	8
15	Dissection-BKW. *Lecture Notes in Computer Science*, **2018**, 638-666	0.9	10
14	Security evaluation and design elements for a class of randomised encryptions. *IET Information Security*, **2019**, 13, 36-47	1.4	3
13	Learning with Physical Noise or Errors. *IEEE Transactions on Dependable and Secure Computing*, **2020**, 17, 957-971	3.9	2
12	Silver: Silent VOLE and Oblivious Transfer from Hardness of Decoding Structured LDPC Codes. *Lecture Notes in Computer Science*, **2021**, 502-534	0.9	12
11	On the Sample Complexity of solving LWE using BKW-Style Algorithms. **2021**,		1
10	Adventures in Crypto Dark Matter: Attacks and Fixes for Weak Pseudorandom Functions. *Lecture Notes in Computer Science*, **2021**, 739-760	0.9	1
9	Towards Sound Fresh Re-keying with Hard (Physical) Learning Problems. *Lecture Notes in Computer Science*, **2016**, 272-301	0.9	13
8	Optimization of (mathsf {LPN}) Solving Algorithms. *Lecture Notes in Computer Science*, **2016**, 703-728	0.9	12
7	On the Complexity of the LWR-Solving BKW Algorithm. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, **2020**, E103.A, 173-182	0.4	
6	BKW Meets Fourier New Algorithms for LPN with Sparse Parities. *Lecture Notes in Computer Science*, **2021**, 658-688	0.9	1
5	Adventures in crypto dark matter: attacks, fixes and analysis for weak pseudorandom functions. *Designs, Codes, and Cryptography*,	1.2	
4	Modeling and simulating the sample complexity of solving LWE using BKW-style algorithms.		
3	Calibrating Learning Parity with Noise Authentication for Low-Resource Devices. **2022**, 19-36		0

2	Correlated Pseudorandomness from Expand-Accumulate Codes. **2022**, 603-633	2
1	A Non-heuristic Approach to Time-Space Tradeoffs and Optimizations for BKW. **2022**, 741-770	0